

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

AMENDMENTS

In the Claims

Claims 1—71 were pending at the time of the Action.

Claims 1—71 are rejected.

No claims are canceled or amended by the current Response.

New claim 72 was added.

Accordingly, claims 1—72 remain pending and are provided herein below in a complete listing of claims for the sake of convenience:

Listing of Claims:

1. (Original) A method comprising:
verifying that a first application is authorized to set an initial range for a controlled parameter setting;
if authorized, allowing the first application to set an initial range for the controlled parameter setting; and
subsequently, allowing at least a second application to modify the controlled parameter setting within the initial range set by the first application.

2. (Original) A method as recited in claim 1, wherein the first application is verified based on a first security code.

1 3. (Original) A method as recited in claim 2, wherein the first
2 security code is at least partially encrypted.

3
4 4. (Original) A method as recited in claim 1, wherein the first
5 application is verified based at least partially on memory location information
6 associated with a verifying function.

7
8 5. (Original) A method as recited in claim 4, wherein the memory
9 location information associated with the verifying function defines memory
10 location within a read only memory (ROM).

11
12 6. (Original) A method as recited in claim 1, wherein the initial
13 range includes at least a maximum controlled parameter setting, and the second
14 application is not allowed to modify the controlled parameter setting beyond the
15 maximum controlled parameter setting.

16
17 7. (Original) A method as recited in claim 1, wherein the initial
18 range includes at least a minimum controlled parameter setting, and the second
19 application is not allowed to modify the controlled parameter setting below the
20 minimum controlled parameter setting.

21
22 8. (Original) A method as recited in claim 1, further comprising:
23 verifying that the second application is authorized to modify a current range
24 for the controlled parameter setting;
25

1 if authorized, allowing the second application to modify the current range
2 for the controlled parameter setting; and

3 subsequently, allowing at least a third application to modify the controlled
4 parameter setting within the current range as modified by the second application.

5
6 **9. (Original)** A method as recited in claim 8, wherein the second
7 application is verified based on a second security code.

8
9 **10. (Original)** A method as recited in claim 9, wherein the second
10 security code is at least partially encrypted.

11
12 **11. (Original)** A method as recited in claim 8, wherein the second
13 application is verified based at least partially on memory location information
14 associated with a verifying function.

15
16 **12. (Original)** A method as recited in claim 11, wherein the memory
17 location information associated with the verifying function defines memory
18 location within a read only memory (ROM).

19
20 **13. (Original)** A method as recited in claim 8, wherein the current
21 range includes at least a maximum controlled parameter setting, and the third
22 application is not allowed to modify the controlled parameter setting beyond the
23 maximum controlled parameter setting.

1 14. (Original) A method as recited in claim 8, wherein the current
2 range includes at least a minimum controlled parameter setting, and the third
3 application is not allowed to modify the controlled parameter setting below the
4 minimum controlled parameter setting.

5
6 15. (Original) A method as recited in claim 1, wherein the controlled
7 parameter setting is selected from a group of settings comprising an audio volume
8 control parameter, an audio tone control parameter, an illumination control
9 parameter, a visual display control parameter, a temperature control parameter, a
10 communication access control parameter, a peripheral device control parameter, a
11 vehicle control parameter, and an environment control parameter.

12
13 16. (Original) A method as recited in claim 8, wherein:
14 verifying that the first application is authorized to set the initial range for
15 the controlled parameter setting further includes using a first verifier; and
16 verifying that the second application is authorized to modify the current
17 range for the controlled parameter setting further includes using a second verifier,
18 wherein the first verifier and the second verifier are operatively configured
19 in a serial arrangement, and the first verifier is independently responsive to a first
20 security code and the second verifier is independently responsive to a second
21 security code.

22
23 17. (Original) A method as recited in claim 16, wherein the first
24 verifier is provided by a first entity and the second verifier that is provided by a
25 second entity.

1
2 **18.** (Original) A method as recited in claim 16, wherein the first
3 security code and the second security code are the same.

4
5 **19.** (Original) A method as recited in claim 16, wherein the first
6 security code is provided by a first entity and the second security code is provided
7 by a second entity.

8
9 **20.** (Original) A method as recited in claim 1, wherein verifying that
10 the first application is authorized to set the initial range for the controlled
11 parameter setting further includes using at least one verifier selected from a group
12 comprising at least a first verifier and a second verifier.

13
14 **21.** (Previously presented) A method as recited in claim 8, wherein
15 verifying that the second application is authorized to set the initial range for the
16 controlled parameter setting further includes using at least one verifier selected
17 from a group comprising at least a first verifier and a second verifier.

18
19 **22.** (Original) A computer-readable medium having computer-
20 executable instructions for performing steps comprising:

21 verifying that a first application is authorized to set an initial range for a
22 controlled parameter setting;

23 if authorized, allowing the first application to set an initial range for the
24 controlled parameter setting; and
25

1 subsequently, allowing at least a second application to modify the
2 controlled parameter setting within the initial range set by the first application.
3

4 **23.** (Original) A computer-readable medium as recited in claim 22,
5 wherein the first application is verified based on a first security code.
6

7 **24.** (Original) A computer-readable medium as recited in claim 23,
8 wherein the first security code is at least partially encrypted.
9

10 **25.** (Original) A computer-readable medium as recited in claim 22,
11 wherein the first application is verified based at least partially on memory location
12 information associated with a verifying function.
13

14 **26.** (Original) A computer-readable medium as recited in claim 25,
15 wherein the memory location information associated with the verifying function
16 defines memory location within a read only memory (ROM).
17

18 **27.** (Original) A computer-readable medium as recited in claim 22,
19 wherein the initial range includes at least a maximum controlled parameter setting,
20 and the second application is not allowed to modify the controlled parameter
21 setting beyond the maximum controlled parameter setting.
22

23 **28.** (Original) A computer-readable medium as recited in claim 22,
24 wherein the initial range includes at least a minimum controlled parameter setting,
25

1 and the second application is not allowed to modify the controlled parameter
2 setting below the minimum controlled parameter setting.

3
4 **29.** (Original) A computer-readable medium as recited in claim 22,
5 having computer-executable instructions for performing steps further comprising:
6 verifying that the second application is authorized to modify a current range
7 for the controlled parameter setting;
8 if authorized, allowing the second application to modify the current range
9 for the controlled parameter setting; and
10 subsequently, allowing at least a third application to modify the controlled
11 parameter setting within the current range as modified by the second application.

12
13 **30.** (Original) A computer-readable medium as recited in claim 29,
14 wherein the second application is verified based on a second security code.

15
16 **31.** (Original) A computer-readable medium as recited in claim 30,
17 wherein the second security code is at least partially encrypted.

18
19 **32.** (Original) A computer-readable medium as recited in claim 29,
20 wherein the second application is verified based at least partially on memory
21 location information associated with a verifying function.

22
23 **33.** (Original) A computer-readable medium as recited in claim 32,
24 wherein the memory location information associated with the verifying function
25 defines memory location within a read only memory (ROM).

1
2 **34.** (Original) A computer-readable medium as recited in claim 29,
3 wherein the current range includes at least a maximum controlled parameter
4 setting, and the third application is not allowed to modify the controlled parameter
5 setting beyond the maximum controlled parameter setting.

6
7 **35.** (Original) A computer-readable medium as recited in claim 29,
8 wherein the current range includes at least a minimum controlled parameter
9 setting, and the third application is not allowed to modify the controlled parameter
10 setting below the minimum controlled parameter setting.

11
12 **36.** (Original) A computer-readable medium as recited in claim 22,
13 wherein the controlled parameter setting is selected from a group of settings
14 comprising an audio volume control parameter, an audio tone control parameter,
15 an illumination control parameter, a visual display control parameter, a
16 temperature control parameter, a communication access control parameter, a
17 peripheral device control parameter, a vehicle control parameter, and an
18 environment control parameter.

19
20 **37.** (Original) A computer-readable medium as recited in claim 29,
21 wherein:

22 verifying that the first application is authorized to set the initial range for
23 the controlled parameter setting further includes using a first verifier; and

24 verifying that the second application is authorized to modify the current
25 range for the controlled parameter setting further includes using a second verifier,

1 wherein the first verifier and the second verifier are operatively configured
2 in a serial arrangement, and the first verifier is independently responsive to a first
3 security code and the second verifier is independently responsive to a second
4 security code.

5
6 **38.** (Original) A computer-readable medium as recited in claim 37,
7 wherein the first verifier is provided by a first entity and the second verifier that is
8 provided by a second entity.

9
10 **39.** (Original) A computer-readable medium as recited in claim 37,
11 wherein the first security code and the second security code are the same.

12
13 **40.** (Original) A computer-readable medium as recited in claim 37,
14 wherein the first security code is provided by a first entity and the second security
15 code is provided by a second entity.

16
17 **41.** (Original) A computer-readable medium as recited in claim 22,
18 wherein verifying that the first application is authorized to set the initial range for
19 the controlled parameter setting further includes using at least one verifier selected
20 from a group comprising at least a first verifier and a second verifier.

21
22 **42.** (Original) A computer-readable medium as recited in claim 29,
23 wherein verifying that the first application is authorized to set the initial range for
24 the controlled parameter setting further includes using at least one verifier selected
25 from a group comprising at least a first verifier and a second verifier.

1
2 **43.** (Original) A method comprising:
3 setting an authorized range and a current value for a controlled parameter;
4 receiving a request to change the current value of the controlled parameter
5 from an application;
6 changing the current value of the controlled parameter if a requested value
7 of the controlled parameter is within the authorized range;
8 otherwise, verifying that the application is authorized to modify the
9 authorized range for the controlled parameter, prior to changing the current value
10 of the controlled parameter to the requested value.

11
12 **44.** (Original) A method as recited in claim 43, wherein verifying
13 that the application is authorized to modify the authorized range for the controlled
14 parameter further comprises changing the authorized range to include the
15 requested value when the application is authorized to modify the authorized range.

16
17 **45.** (Original) A method as recited in claim 44, wherein the
18 authorized range includes at least one authorized limit selected from a group
19 including a minimum authorized limit and a maximum authorized limit.

20
21 **46.** (Original) A method as recited in claim 45, further comprising
22 changing the current value of the controlled parameter to the minimum authorized
23 limit if the requested value is less than the minimum authorized limit and the
24 application is not authorized to modify the authorized range.

25

1 **47.** (Original) A method as recited in claim 45, further comprising
2 changing the current value of the controlled parameter to the maximum authorized
3 limit if the requested value is more than the maximum authorized limit and the
4 application is not authorized to modify the authorized range.

5
6 **48.** (Original) A computer-readable medium having computer-
7 executable instructions for performing steps comprising:

8 setting an authorized range and a current value for a controlled parameter;

9 receiving a request to change the current value of the controlled parameter
10 from an application;

11 changing the current value of the controlled parameter if a requested value
12 of the controlled parameter is within the authorized range;

13 otherwise, verifying that the application is authorized to modify the
14 authorized range for the controlled parameter, prior to changing the current value
15 of the controlled parameter to the requested value.

16
17 **49.** (Original) A computer-readable medium as recited in claim 48,
18 wherein verifying that the application is authorized to modify the authorized range
19 for the controlled parameter further comprises changing the authorized range to
20 include the requested value when the application is authorized to modify the
21 authorized range.

22
23 **50.** (Original) A computer-readable medium as recited in claim 49,
24 wherein the authorized range includes at least one authorized limit selected from a
25 group including a minimum authorized limit and a maximum authorized limit.

1
2 **51.** (Original) A computer-readable medium as recited in claim 50,
3 further comprising computer-executable instructions for performing the step of
4 changing the current value of the controlled parameter to the minimum authorized
5 limit if the requested value is less than the minimum authorized limit and the
6 application is not authorized to modify the authorized range.

7
8 **52.** (Original) A computer-readable medium as recited in claim 50,
9 further comprising computer-executable instructions for performing the step of
10 changing the current value of the controlled parameter to the maximum authorized
11 limit if the requested value is more than the maximum authorized limit and the
12 application is not authorized to modify the authorized range.

13
14 **53.** (Original) A system comprising:
15 at least one processor operatively configured to respond to computer
16 instructions associated with a plurality of applications, including a first
17 application;
18 memory coupled to the processor and configured to store data associated
19 with at least the first application, and
20 a program operatively configured within the processor and memory and
21 arranged to set a parameter value and a range associated with at least one
22 controlled parameter, determine if the first application is authorized to modify the
23 range, modify the parameter value within the range when requested by the first
24 application, and modify the parameter value outside the range and modify the
25

1 range when requested by the first application if the first application is authorized
2 to modify the range.

3
4 **54.** (Original) A system as recited in claim 53, wherein the program
5 determines if the first application is authorized to modify the range by analyzing a
6 security code provided by the first application.

7
8 **55.** (Original) A system as recited in claim 54, wherein the program
9 decodes the security code and compares the resulting data to predetermined data to
10 determine if the first application is authorized to modify the range.

11
12 **56.** (Original) A system as recited in claim 54, wherein the program
13 determines that the first application is authorized to change the range only if the
14 security code matches a valid security code.

15
16 **57.** (Original) A system as recited in claim 54, wherein the program
17 further includes at least one linked verifier function stored within a predefined
18 portion of the memory, and the program is configured to determine if the linked
19 verifier function, as called by the program, is not within the predefined portion of
20 the memory, in which case, the program determines that the first application is
21 unauthorized to modify the range.

22
23 **58.** (Original) A system as recited in claim 57, wherein the
24 predefined memory location is within a read only portion of the memory.
25

1 **59.** (Original) A system as recited in claim 54, wherein the security
2 code is uniquely associated a software developer entity responsible for providing
3 the first application.
4

5 **60.** (Original) A system as recited in claim 53, wherein the processor
6 is operatively configured to respond to computer instructions associated with at
7 least a second application, and the program is further configured to determine if
8 the second application is authorized to modify the range, modify the parameter
9 value within the range when requested by the second application, and modify the
10 parameter value outside the range and modify the range when requested by the
11 first application if the first application is authorized to modify the range.
12

13 **61.** (Original) A system as recited in claim 53 wherein the parameter
14 is selected from a group comprising an audio volume control parameter, an audio
15 tone control parameter, an illumination control parameter, a visual display control
16 parameter, a temperature control parameter, a communication access control
17 parameter, a peripheral device control parameter, a vehicle control parameter, and
18 an environment control parameter.
19

20 **62.** (Original) A system as recited in claim 53, wherein the processor,
21 the memory, and the program are part of a computer system within a vehicle.
22

23 **63.** (Original) A system as recited in claim 53, further comprising at
24 least one device that is coupled to the program and is responsive to the parameter
25 value from the program.

1
2 **64.** (Original) An arrangement for use in a computer system, the
3 arrangement comprising:

4 a parameter manager configurable to receive a parameter change request
5 from one or more computer applications and selectively output a corresponding
6 parameter value;

7 at least one verifier function accessible by the parameter manager and
8 configured to determine if the parameter change request is from a computer
9 application that is authorized to exceed a parameter limitation; and

10 a device driver coupled to the parameter manager and configured to receive
11 the parameter value from the parameter manager and output a corresponding
12 control parameter suitable for use by at least one device.

13
14 **65.** (Original) An arrangement as recited in claim 64, wherein the
15 verifier determines if the parameter change request is from the computer
16 application authorized to exceed the parameter limitation by analyzing a security
17 code identified by the first application.

18
19 **66.** (Original) An arrangement as recited in claim 65, wherein the
20 verifier decodes the security code and compares the resulting data to a valid
21 security code to determine if the computer application is authorized to exceed the
22 parameter limitation.

23
24 **67.** (Original) An arrangement as recited in claim 65, wherein at least
25 a portion of the verifier is invoked by the parameter manager in a predefined,

1 identifiable manner, such that if invoked otherwise the computer application is
2 deemed unauthorized to exceed the parameter limitation.

3
4 **68.** (Original) An arrangement as recited in claim 67, further
5 comprising a memory, and wherein the at least a portion of the verifier that is
6 invoked by the parameter manager in a predefined, identifiable manner is
7 associated with at least one memory location within a read only portion of the
8 memory.

9
10 **69.** (Original) An arrangement system as recited in claim 64, wherein
11 the security code is uniquely associated a software developer entity responsible for
12 providing the computer application and the verifier.

13
14 **70.** (Original) An arrangement as recited in claim 64, wherein the
15 parameter manager, verifier, and device driver are part of a computer system
16 within a vehicle.

17
18 **71.** (Original) An arrangement as recited in claim 64, wherein the at
19 least one device includes a computer implemented function.

20
21 **72.** (New) An arrangement as recited in claim 64, wherein the parameter
22 manager is configured to change the corresponding parameter value to a minimum
23 authorized limit if the parameter change request is less than the minimum
24 authorized limit and the verifier function determines the computer application is
25 not authorized to modify the parameter limitation.